AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

Ra'i-Arii Mariteragi,

Defendant.

Case No. 2:25-MJ-03800-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date of June 20, 2025, in the county of Los Angeles in the Central District of California, the defendant violated:

Code Section	*Offense Description*
21 U.S.C. § 841(a)(1)	Possession with Intent to Distribute Methamphetamine

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/
Complainant's signature

Andrew Youssef, HSI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. m . 4.1 by 1 phone.

Date: 6/22/25

Judge's signature

City and state: Los Angeles, California

Hon. Brianna Mircheff, U.S. Magistrate Judge
Printed name and title

AUSA: Mirelle Raza x6058

AFFIDAVIT

I, Andrew Youssef, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against Ra'i-Arii MARITERAGI ("MARITERAGI"), for a violation of Title 21 U.S.C. § 841(a)(1) (possession with intent to distribute methamphetamine).

2. This affidavit is also made in support of an application for a warrant to search the following digital device seized from MARITERAGI'S belongings, and currently in the custody of Homeland Security Investigations ("HSI") in El Segundo, California, and described more fully in attachment A:

a. A white colored Apple iPhone, Passcode: "654321" (the "SUBJECT DEVICE");

3. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances), 21 U.S.C. § 846 (conspiracy to possess with the intent to distribute controlled substances), 21 U.S.C. § 953(a) (unlawful exportation of controlled substances), 21 U.S.C. § 960 (knowing exportation of a controlled substance), and 18 U.S.C. § 554 (knowing exportation of any merchandise contrary to any law) (the "Subject Offenses"), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and databases. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and warrant, and does not purport to set forth all my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only, all amounts or sums are approximate, and all dates and times are on or about those indicated.

II. BACKGROUND OF AFFIANT

5. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations ("HSI"), where I have worked since September of 2024. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(c), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. In the course of my work, I have conducted physical surveillance and reviewed electronic records.

6. During my tenure as a Special Agent, I have completed approximately six months of instruction at the Federal Law Enforcement Training Center, in Glynco, Georgia, completing the Criminal Investigator Training Program and HSI's add on training, HSI Special Agent Training. Prior to my tenure as a Special Agent, I was a Legal Assistant with the United States

Attorney's Office in the Central District of California for approximately eight months, from February to September 2024. Additionally, prior to being a Legal Assistant, I was a Student Trainee with the United States Attorney's Office for approximately one and a half years, from September 2022 to February 2024. Additionally, I hold a Bachelor of Science degree in Criminology and Criminal Justice, and certification in Crime Scene Investigation from California State University, Long Beach.

IV. STATEMENT OF PROBABLE CAUSE

7. Based on my involvement in this investigation, my conversations with other law enforcement officials involved in this investigation, and my review of reports and records connected to this investigation, I am aware of the following:

8. MARITERAGI was scheduled to fly from Los Angeles International Airport ("LAX") to Tahiti Faa'a International Airport on Air Tahiti Flight TN 101 on June 20, 2025, at approximately 11:55 p.m.

9. At approximately 10:33 p.m., MARITERAGI entered the body scanner at the Transportation Security Administration ("TSA") checkpoint lane #8, and the scan revealed that he had an anomaly in his groin area.

10. TSA Officers asked MARITERAGI what he was concealing in the groin area of his pants, and MARITERAGI stated he had nothing in his pants. TSA officers took MARITERAGI to a private screening area to further investigate the anomaly. TSA officers advised MARITERAGI that the police were going to be called if

he did not comply. MARITERAGI then revealed that he was concealing an object underneath his pants, and three undergarments of clothing. The object was wrapped in plastic wrap.

11. TSA officers immediately notified their management and the Los Angeles International Airport Police Department ("LAX PD"). TSA officers ran the object through the X-ray machine, revealing an inorganic mass.

12. At approximately 10:50 p.m., LAX PD received a radio call from TSA regarding a narcotic investigation in TSA's private screening room. LAX PD officers arrived at the scene to meet MARITERAGI at approximately 11:00 p.m.

13. LAX Officers cut through a portion of the package revealing a white crystalized substance. Customs and Border Protection ("CBP") and HSI were notified and arrived on scene for further investigation. CBP Officer Marionette Ventrice conducted a field test of the white crystalized substance using a Thermo Scientific Gemini Analyzer. The field test showed a positive match for methamphetamine.

14. At approximately 11:35 p.m., the HSI LAX Duty Agent was contacted by LAX PD regarding MARITERAGI. HSI LAX arrived on scene and took custody of MARITERAGI and the drugs.

15. On June 21, 2025, HSI Special Agents arrived at Hawthorne Police Department, where MARITERAGI was being temporarily held, to conduct a subject interview. Prior to the interview, a French translator was contacted and utilized to aid with the interview.

16. At approximately 12:01 p.m. MARITERAGI was read his Miranda Rights. MARITERAGI agreed to waive his rights and signed the Miranda Waiver form. During the interview, MARITERAGI admitted to purchasing the methamphetamine in the Anaheim area for approximately $965. MARITERAGI admitted that his intention was to smuggle the drugs into LAX for the purpose of transporting them to Tahiti for distribution. The interview ended at approximately 1:16 p.m.

III. TRAINING AND EXPERIENCES ON DRUG OFFENSES

17. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package, and deliver the drugs and launder the drug proceeds. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities in order to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds.

b. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. The aforementioned records are often maintained where the drug trafficker has ready access to them, such as on their cell phones and other digital devices.

c. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of the drugs between the seller and the buyer, the negotiation of price, and discussion of whether or not participants will bring weapons to a deal. In addition, it is common for people engaged in drug trafficking to have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

d. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices. Drug traffickers often keep records of meetings with associates, customers, and suppliers on their digital devices, including in the form of calendar entries and location data.

IV. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[1]

18. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have

[1] As used herein, the term "digital device" includes SUBJECT DEVICE.

been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain

software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

19. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it can take a substantial period of time to search a digital device for many reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

20. The search warrant requests authorization to use the biometric unlock features of a device, based on the following,

which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. The person who is in possession of a device or has the device among his or her belongings is likely a user of the device. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress MARITERAGI's thumb and/or fingers on

the device; and (2) hold the device in front of MARITERAGI's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

V. CONCLUSION

21. For all the reasons described above, I submit that there is probable cause to believe that MARITERAGI has committed a violation of Title 21 U.S.C. § 841(a)(1) (possession with intent to distribute methamphetamine). I further submit that there is probable cause to believe that the items to be seized described in Attachment B will be found in a search of the SUBJECT DEVICE, described in Attachment A.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 22nd day of June 2025.

HON. BRIANNA MIRCHEFF
UNITED STATES MAGISTRATE JUDGE